Unprecedented

Space-based Information in Operation Iraqi Freedom

By LTC Max Corneau

LTC Max Corneau is a mobilized reservist supporting the Amry Strategic Space Information Operations Element. He served 16 years on active duty as a special electronic mission aircraft pilot and SIGINT officer. He served throughout the world in five Aerial Exploitation battalions and was the Army's first Aviation officer to be instructor qualified on the E-8C JSTARS aircraft. He served in a direct support role to Operation Iraqi Freedom and flew combat surveillance missions in Operations Noble Anvil and Desert Storm.

Combat Operation Iraqi Freedom (OIF) was characterized by an unprecedented reliance on Space-based information systems. U.S. forces relied heavily on Space-based communications, as did the Iraqi regime and regional governments who had a stake in the outcome. In all cases, combatant forces leveraged commercial Space systems to further their individual objectives. In addition, global media organizations dispatched and assembled to cover the war were equipped with a variety of Space-based voice, data, and live video systems capable of broadcasting to a worldwide audience as events unfolded. In all these use cases, coalition, Iraqi regime, contiguous governments, and media operations depended on Space-based information to meet their objectives.

This article describes information activities and kinetic "information" targeting in OIF, followed by a look at recent state and non-state sponsored attacks against Space systems. Finally, within the context of Department of Defense Space Directives and the Army Space Policy, the article seeks to highlight the implications of our nation's increasing reliance on Space information through all phases of conflict.

Before beginning, a review of current Space policy is in order. According to the April 2003 Army Space Policy: "Space dominance and the full exploitation of space-based systems are vital to achieving the precision, information superiority and battle command capabilities essential for executing the responsive, full spectrum, distributed operations envisioned for Land Force units." The policy statement continues that future information flow to military decision makers will approach near-real-time as commercial and military uses of Space accelerate. To support its objectives, the Space Policy further states: "The Army must promote a federated and distributed information network of sensors and communication devices among Commercial, Military, and National Space-Based Capabilities as part of the Global Information Grid." Keep this in mind as you read the following.

Space-Based Information in OIF

U.S. Forces

During OIF, U.S. forces relied heavily on Space-based communications. According to Air Force Secretary James Roche, in an address to the 19th Annual National Space Symposium in Colorado Springs, Colo. in April 2003, there was insufficient bandwidth to support signals among ships, troops, commanders, and aircraft. Roche said, "We consumed an awful lot of bandwidth. We rent as much bandwidth as we can get our hands on and we're trying to become more efficient." Echoing Roche's sentiments, LTG Peter Cuviello, the Army's Chief Information Officer highlighted the extraordinary amount of commercial communications used in OIF. "About 80 percent of our capability over there (southwest Asia) was commercial satellite. When U.S. troops go back to home station, they don't have that capability."

One example of U.S. use of commercial systems can be seen in its $36 million annual contract with Iridium Satellite, LLC to deliver unlimited minutes to 20,000 users. According to Iridium, Department of Defense (DoD) traffic increased threefold in the months prior to OIF. The federal government owns its own Iridium ground station. Iridium usage by the DoD is part of a methodical plan to provide mobile, global communications to select forces.

DoD use of commercial systems is fraught with risks when not managed properly, from tactical, technical, and operational views. In April 2003, U.S. Central Command (CENTCOM) banned the use of more than 500 Thuraya phones in use by its combatant forces and accompanying embedded media. Thuraya is a telecommunications company based in the United Arab Emirates. The handheld, dual-mode phones apply global positioning system (GPS) technology and are considered a security risk by

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2003**	2. REPORT TYPE	3. DATES COVERED **00-00-2003 to 00-00-2003**
4. TITLE AND SUBTITLE **Unprecedented. Space-based Information in Operation Iraqi Freedom**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Space & Missile Defense Command,Army Forces Strategic Command,Redstone Arsenal,AL,35809**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

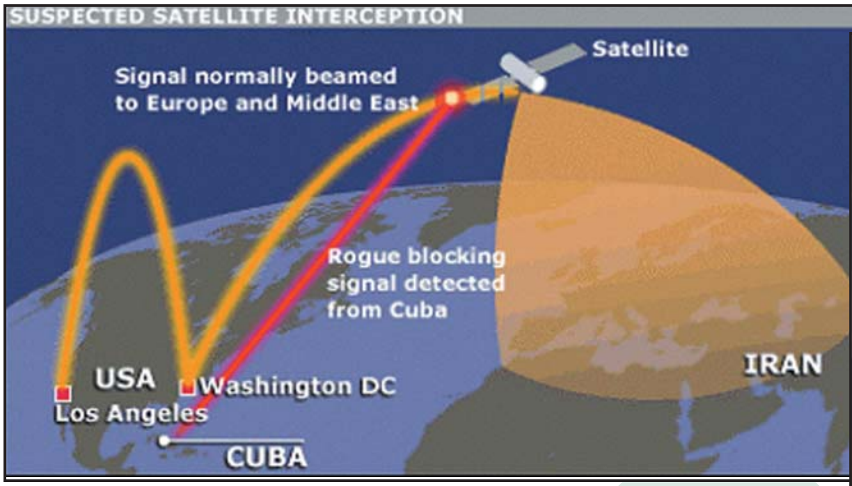
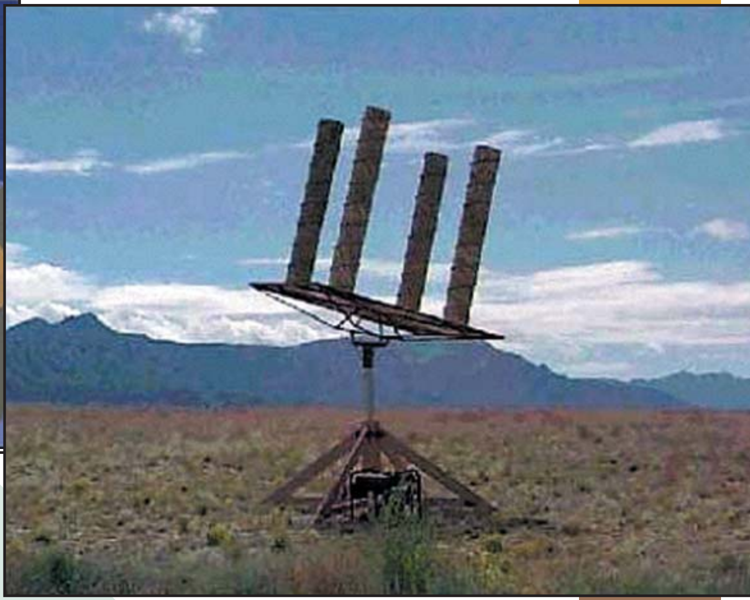

SUSPECTED SATELLITE INTERCEPTION
Satellite
Signal normally beamed to Europe and Middle East
Rogue blocking signal detected from Cuba
IRAN
USA
Washington DC
Los Angeles
CUBA

Figure 1 Global Nature of Interference (courtesy BBC)



The $7,500 Swap Meet UHF Jammer

U.S. officials. GPS data gathered by the Thuraya system is downloaded at the company headquarters in the United Arab Emirates and could be made available to third parties since this station is not under U.S. control.

Global Media

OIF was also characterized by the most robust and pervasive near-real-time battlefield reporting in history. Reporters embedded with U.S. forces used satellite technology to provide global minute-by-minute reports as battles were joined. The restriction on Thuraya phones adversely affected some reporters, but the journalist's kitbag usually consisted of a variety of information tools. Generally, the largest unit in use by reporters in Iraq was the INMARSAT M-4 Communicator. This 10-pound, $8,000 unit provided 48 photos per hour. The SwiftLink system, riding an INMARSAT link provided the majority of video coverage across a 128 KBpS link.

In stark contrast to the coverage provided by U.S. embedded reporters, the Al Jazeera satellite TV network provided global images of captive and killed U.S. servicemembers, as well as civilian casualties. And who can ever forget the images of "Baghdad Bob" Mohammed Said al-Sahaf exhorting Jihadists and martyrs to fight the American infidels, as he called them, in any way possible. Recall that Baghdad Bob's press conferences usually originated from Iraq's state owned satellite TV channel, the Iraqi Satellite Channel.

Kinetic Information Targets

U.S. CENTCOM's OIF target list included command and control targets. One of these intended targets was the group of buildings in Baghdad housing the Baghdad satellite communications, according to a CNN report filed on March 26 after Coalition Tomahawk missiles struck the facility. According to the report, which cited CENTCOM officials, the March 26 Tomahawk strike was aimed at eliminating the system used by the regime to communicate with troops and the Iraqi people. The day before the Tomahawk attack, Iraqi television aired footage of five U.S. prisoners of war that included four dead U.S. soldiers lying crumpled and bloodstained in a makeshift morgue. The Iraqi footage was very powerful — aired by several Arab satellite media outlets, it was not generally carried by U.S. media sources. Clearly, the Iraqi regime intended to use its satellite communications capabilities for military command and control, as well as propaganda to the world. The regime's Ministry of Information was struck successfully a second time on March 31 in a continuing effort to reduce the Hussein regime's command and control capabilities.

Looking Back and Forth

We hope that a clear picture is emerging that shows U.S. forces relying heavily on commercial Space information. In addition to combatant use of Space systems, global media rely on Space information systems to report on war and newsworthy conflict. Finally, we see in OIF that the Iraqi regime relied on Space information to command and control its forces, as well as communicate its message to the rest of the world. This reliance fostered the importance given to its systems by U.S. forces.

Space Information Warfare Past and Present

Geostationary orbit (22,300 miles high over the equator) is no longer a safe place. This haven for communication satellites orbiting over a fixed point on the Earth's surface is filled with hackers, crackers, jammers, pirates, and angry people. Let's chronologically examine some recent Space information operations whose perpetrators and targets span the globe.

Indonesia and Tonga

(See Unprecedented , page 63)

Unprecedented ... from Page 49

Indonesia has admitted jamming the APSTAR 1A satellite components operated by Tonga. The jamming resulted from a dispute over who owns the sought after orbital 134 degree east longitude slot over the equator linking the Pacific and Asia. The dispute dates back to a meeting in late October 1993 when delegates met to resolve the issue. Tonga claims registration rights to the slot, while Indonesia believes the agreement reached in 1993 gives them indefinite rights to the 134E slot.

Turkey and the Kurds

In 1998, according to the Sabah newspaper published in Turkey, the Turkish government took responsibility for jamming the Kurdish language broadcast on Med-TV satellite channel. In August 1997, the same channel, carried aboard the EUTELSAT was jammed for three weeks by the Turkish government.

China and the Falun Gong

In September 2002, China complained that during the previous weeks its SINOSAT satellite TV system had been regularly hijacked by signals coming from Taiwan. In 1999 China declared the Falun Gong an "evil cult" and outlawed its existence. Evidently, the Falun Gong has sought haven on Taiwan to beam its message to the Chinese mainland. To avoid future satellite piracy, China is outfitting its systems aboard the French-built APSTAR VI satellite with a powerful anti-jamming capability. APSTAR VI is slated for launch in late 2004.

U.S., Cuba and Iran

The most recent, and pertinent, transnational Space war began in July 2003 and involves a jamming source originating from Cuba against a U.S. satellite that is broadcasting information into Iran. In a complex set of links and nodes (Figure 1., page 49) the Los Angeles-based ParsTV, Azadi, and Appadana Television are uplinked from California via the TELSTAR-5 satellite. This signal arrives at the Washington international teleport and is further uplinked to the TELSTAR-12 satellite over the eastern Atlantic Ocean and broadcast into Iran across the Voice of America (VOA) network. The TELSTAR-12 uplink is being jammed. According to a letter from Loral (the TELSTAR operator), the interference began at 5:35 p.m. on July 5, shortly after the start of VOA broadcasts.

Loral determined that the interference was caused by a third party and asked a separate commercial firm, Transponder Location Services (TLS) of Chantilly, Va., to attempt to locate the source of the interference. TLS determined the probable source of the interference as Havana, Cuba.

Countering the Threat: Commercial SATCOM Interference Geolocation

Transponder Location Services (http://www.TLS2000.com) touts itself as a leader in protecting against satellite interference, unauthorized transponder use, and intentional disruption. TLS applies radio interferometry (time difference of arrival of a signal at different locations) to passively and accurately locate unauthorized users and interferers. According to its Web site, TLS has investigated more than 7,000 incidents since its formation. In 1996, the company added a heliborne geolocation capability known as Final SearchTM to pinpoint signal origins. Apparently there are a lot more incidents than the commercial Space-based information providers are willing to share with us. Remember, these information providers are in the business to make money and any reports that their systems are providing less than 100 percent service will adversely affect their revenue streams. So just like companies don't like to admit their computers got hacked and millions of dollars stolen, information providers don't like to admit their vulnerabilities.

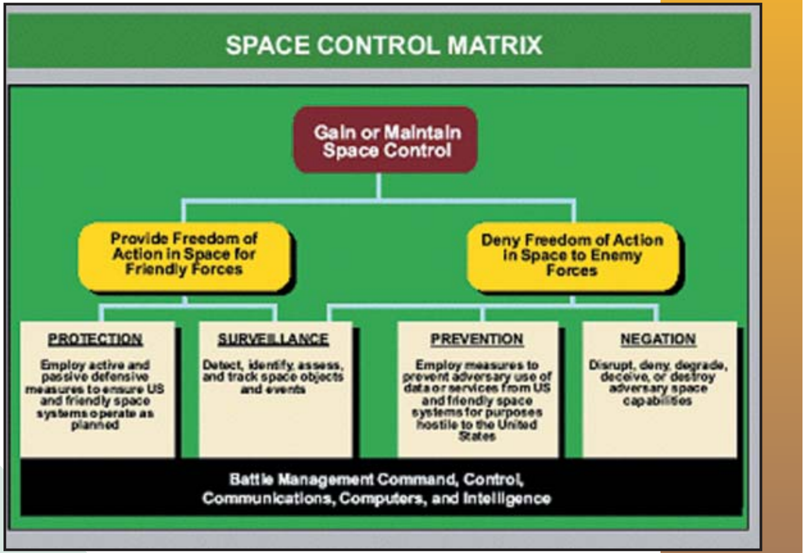

SPACE CONTROL MATRIX
Gain or Maintain Space Control
Provide Freedom of Action in Space for Friendly Forces
Deny Freedom of Action in Space to Enemy Forces
PROTECTION
Employ active and passive defensive measures to ensure US and friendly space systems operate as planned
SURVEILLANCE
Detect, identify, assess, and track space objects and events
PREVENTION
Employ measures to prevent adversary use of data or services from US and friendly space systems for purposes hostile to the United States
NEGATION
Disrupt, deny, degrade, deceive, or destroy adversary space capabilities
Battle Management Command, Control, Communications, Computers, and Intelligence

Figure 2

In the case of the recent VOA broadcast being jammed out of Cuba, according to BBC technical analyst Martin Peters, changing satellites is not the answer as the audience would need to know about this, move their (satellite) dishes and retune their receivers. Peters described Cold War cat and mouse games where western broadcasters would simultaneously use as many frequencies as possible because Russia had only so many transmitters for blocking signals.

And Now the Bad News

The bad news is that just like hacking, Space information warfare has become an active underground battle that fills the Internet with "how-to" guides. I shall not proliferate such information here, but suffice it to say that a brief search revealed a lot of information. One article begins with an introduction to orbitology and pointing, then details the satellite transmit and receive chains, explains how transponders work and details frequency pairing.

Another article explained that for $7,500 a small group of young amateurs built a high-powered UHF

SATCOM jammer using wood, plastic, copper tubing, and some electronics purchased at a swap meet.

Implications for a Space-Based Military

So what does all this mean to the U.S. Army and in particular its Space forces? On the continuum of Space Control, we are now focusing on the Protect element (Figure 2). Thus far, this article established that the U.S. military relied heavily on Space information systems during OIF and that commercial Space systems are under heavy attack from nation states, transnational actors, Space-hackers, and criminals. Now let's put it together and see what it means and what we can do to ensure our freedom of action in Space as specified in DoD Directives and Army Space Policy.

Blue-Gray-Red Systems

The security and cooperative nature of Space information systems and owner/operators varies tremendously. U.S. military secure Space information systems maintain robust protection and countermeasures and are controlled solely by U.S. forces. Next in line are the cooperative commercial systems such as Iridium where the commercial operator maintains the Space segment, but U.S. forces have a dedicated ground station under our control. Least secure are the commercial systems operated solely by commercial entities, especially those operators who may not be able to defend our interests, such as Thuraya. A concerted effort must be made to plan ahead and avoid using the category of systems such as Thuraya.

Protecting against Hacks

Given that the military will rely heavily on commercial systems for the foreseeable future, we must take steps to defend ourselves. One way to protect ourselves is to develop a system of alerts and warnings that spans from the first line of defense to the Space information system consumer to the ground system operator. A metaphor for such defense already exists in the computer network domain where operators through global network managers receive immediate warnings when malicious computer code is afoot. To accomplish this, operators must know how to identify and report service interference or denials. Additionally, a dedicated Space information awareness network could be applied at the management level to respond defensively.

The Civil Reserve Air Fleet Model

A significant part of the nation's air mobility resides with the Civil Reserve Air Fleet (CRAF). Selected aircraft from U.S. airlines, contractually committed to CRAF, support DoD airlift requirements in emergencies when the need for airlift exceeds the capability of military aircraft.

Participating airlines contractually pledge aircraft to the various segments of CRAF, ready for incremental activation when needed. To provide incentives for civil carriers to commit aircraft to the CRAF program and to assure the Unites States of adequate airlift reserves, the government makes peacetime airlift business available to civilian airlines that offer aircraft to the CRAF. DoD offers business through the International Airlift Services, which is the largest contract. For fiscal 2003, the guaranteed portion of the contract is $394 million.

The commander, U.S. Transportation Command, with approval of the secretary of defense, is the activation authority for all three stages of CRAF. When notified of call-up, carriers must meet specific readiness timelines.

The CRAF model could be applied to commercial carriers as follows:

- Commander U.S. Strategic Command would be the activation authority.
- Candidate systems would be identified and offered contracts to support U.S. military contingencies.
- Business incentives in the form of contracts and utilization would make participation compatible with a reasonable business model.
- An incremental activation plan provides for Space information system tailoring.
- U.S. forces modify major operational plans based on a prescribed level of commercial Space information system augmentation.

Summary

To an unprecedented degree, the military relies on commercial Space information systems to accomplish its assigned missions. The commercial Space information world is fraught with danger and malicious potential. Rather than be subjected to these dangers, we must embrace the future as an adaptive force of thinking leaders and operators to assure our access to the ultimate high ground: SPACE.

Endnotes:

1. http://www.cndyorks.gn.apc.org/news/articles/iraq/satelliteshelp.htm. Pam Zubeck. April 13, 2003
2. http://www.nationaldefensemagazine.org/article.cfm?ID=1147. Sandra Irwin. July 2003.
3. http://www.iridium.com/corp/iri_corp-news.asp?newsid=58. Mesa Tribune. April 14, 2003.
4. http://www.msnbc.com/news/895005.asp?0sl=-13. MSNBC News, Reuters. April 13, 2003.
5. http://www.newsandtech.com/issues/2003/05-03/ot/05-03_satellite.htm. Hays Goodman. May 2003.
6. http://foi.missouri.edu/jourwarcoverage/studyincontrasts.html. Raid Qusti. March 26, 2003.
7. http://www.rnw.nl/realradio/features/html/tv030403.html.
8. http://www.news24.com/news24/world/iraq/0,,2-10-1460_1338455,00.html. March 26, 2003.
9. http://spacewar.com/2003/030331074239.bvhmk0q0.html. March 31, 2003.
10. http://www.tongatapu.net.to/tonga/news/briefs/ss970227.htm. February 27, 1997.
11. http://www.cogsci.ed.ac.uk/~siamakr/Kurdish/KURDICA/1998/NOV/MED-letter.html. Kurdish Language and Linguistics Committee. October 16, 1998.
12. http://www.abc.net.au/news/newsitems/s710482.htm. ABC Newsonline. October24, 2002.
13. http://www.live103.com/print.php?sid=87. Robert Windrem. July 12, 2003.
14. http://news.bbc.co.uk/2/hi/americas/3077303.stm
15. http://www.af.mil/news/factsheets/Civil_Reserve_Air_Fleet.html (March 2003)